REMARKS/ARGUMENTS

Favorable reconsideration of this application is respectfully requested.

Claims 41-43, 45, 50-63, 65, and 70-80 are pending in this application. Claims 44, 46-49, 64, and 66-69 are canceled by the present response without prejudice. Claims 41-42, 44, 46-62, 64, and 66-80 were rejected under 35 U.S.C. § 103(a) as unpatentable over U.S. patent 6,453,419 to Flint et al. (herein "Flint") and further in view of U.S. patent 6,609,198 to Wood et al. (herein "Wood"). Claims 43, 45, 63, and 65 were rejected under 35 U.S.C. § 103(a) as unpatentable over Flint and Wood and further in view of the Microsoft Computer Dictionary, 5th Ed. (herein "Microsoft Dictionary").

Addressing the above-note rejections, those rejections are traversed by the present response.

Initially, applicants note each of independent claims 41 and 61 is amended by the present response to clarify features recited therein. Specifically, independent claim 41 now clarifies determining the level of security of the computer network connection based on whether the computer network connection is encrypted, and "wherein a first level of security is set when it is determined that the computer network connection is encrypted and a second level of security is set when it is determined that the computer network connection is not encrypted". Independent claim 41 now also recites that a level of access of the computing device to the network resources is controlled such that the computing device is only allowed access to the first set of network resources, which include a file server, when the first level of security, i.e. an encrypted connection, is determined, and is not allowed access to the first set of network resources but is allowed access to the second set of network resources, which include access to the Internet and an email server, when a second level of security, i.e. a non-encrypted connection, is determined. Independent claim 61 now also recites similar limitations.

As shown in Figure 1A in the present specification as a non-limiting example, different computing devices 2, 6 can be connected to an intermediate device 10. The claimed invention has as an operation to control the access of those computing devices 2, 6 to resources on the network 12A based on how the computing devices 2, 6 connect to the intermediate device 10. With reference to Figure 2A in the present specification as a non-limiting example, if either of the computing devices 2, 6 connect to the intermediate device 10 through an encrypted connection, driver 54 is activated and a firewall setting for level 1 access is provided. In that case a high level of access to various network resources, including a file server, can be provided.[1] Alternatively, if no encryption is utilized for the connection between either of the computing devices 2, 6 and the intermediate device 10, the driver 56 is activated and a firewall setting for level 2 access is utilized. In that case a user may only have a limited access to resources, including the Internet and an email server, on the network.[2] In both cases the user has access to network resources, but that access is more restricted for the level access.

In such ways, in the claimed invention, a security level of a network connection between the computing device and the intermediate device can control the level of network resources available to the computing device. The features recited in the claims are believed to clearly distinguish over the applied art.

Flint is cited with respect to certain above-noted claim features. However, applicants respectfully submit Flint does not disclose or suggest the above-noted features particularly clarified in independent claims 41 and 61. Flint merely discloses that in one feature therein a non-encrypted connection can result in ***no access to a computer network***. The claims have a

[1] See for example the present specification at page 6, lines 10-15.
[2] See for example the present specification at page 6, lines 15-26.

different structure in that in the claims a non-encrypted connection still gives rise to access to resources on the network, including the Internet and an email server.

In further detail, Flint discloses the use of a filter 72 such as in Figure 4 therein. Flint discloses that the filter can be an encryption filter and "the encryption filter requires that a connection is encrypted with a certain level of encryption. It will be up to the user level process to verify that the requirements of the filter are met. If the requirements are not met the ***action is to deny the connection***". (Flint at column 11, lines 58-62, emphasis added).

From the above-noted disclosure it is clear that in Flint the filter is provided to merely deny a connection to a network for example if an encryption connection is not utilized.

The claims have a different operation than that in Flint. In the claims connection to a network can still be provided even if a lower level non-encrypted connection is utilized. However in the claims such a lower level non-encrypted connection results in a different level of access to network resources.

The features clarified in independent claims 41 and 61 are features such as presented in previously pending dependent claims 44 and 46-48, although the claim language is somewhat clarified. The language as recited in each of previously pending claims 44 and 46-48 was noted in the Office Action as met by the disclosure in Flint. However, applicants respectfully submit Flint fails to teach or suggest such features.

With specific reference to the disclosures in Flint, at col. 3, line 48 to col. 4, line 1 and col. 11, lines 58-59,[3] Flint merely discloses the use of firewalls and encryption. However, at no point therein does Flint disclose or suggest the features clarified in the claims in which when a connection to a computer network is via an encrypted connection, the connecting device can access first resources including a file server, but when the connecting device

[3] Those are the disclosures in Flint cited with respect to determining a security level of a computer network connection; see the Office Action of December 1, 2005, top of page 3.

connects via a non-encrypted connection, the connecting device can access second network resources including the Internet and the email server, and cannot access the first set of resources, i.e. cannot access the file server.

Further, at the further noted disclosures in Flint at col. 3, lines 3-63, col. 3, lines 45-46, and column 6, line 9,[4] Flint also does not disclose or suggest features cited with respect to the claimed features. At col. 3, lines 45-46 Flint merely makes a broad statement that sales can come in over the Internet, and are therefore not trusted. That disclosure in Flint does not provide any teaching or suggestion of a device that connects via an encrypted or non-encrypted connection affecting the resources that the device can access, and particularly one of the resources being access through the Internet. The input of sales information via the Internet as noted in Flint is completely unrelated to such claimed features.

According to features clarified in the claims, if a first encrypted connection is made from a computing device, that computing device can have access to a first level of network resources, including a file server. If a second non-encrypted connection is made by the computing device, that computing device only has a more limited access to a second set of network resources, including access to the Internet and an email server.

The relied upon disclosures in Flint do not address the claimed features.

Moreover, applicants respectfully submit no teachings in Wood cure the deficiencies in Flint.

Wood is directed to a completely different device than in Flint. That is, Wood is directed to a device that allows multiple accesses to a network based on trust-levels. Flint is not directed to any such type device.

[4] Those are the disclosures in Flint cited with respect to previously pending dependent claims 46-48; see the Office Action of December 1, 2005, page 5.

Moreover, the teachings in Wood are also not at all directed to controlling the access of different resources based on whether a connection is via an encrypted or non-encrypted connection, in particular such that an encrypted connection allows access to a file server, and a non-encrypted connection does not allow access to a file server, but allows access to the Internet and an email server. Such specific features recited in the claims are believed to be clearly neither taught nor suggested by Wood. Thus, Wood cannot cure the deficiencies of Flint discussed above.

In maintaining the outstanding rejection the outstanding Office Action also cites the disclosure in Flint at col. 2, lines 15-28 with respect to one or more services bridging first and second regions.[5] That broad disclosure in Flint does not, however, disclose any of the specific features clarified in the claims, specifically the determination whether a connection to a computer network is via an encrypted connection or a non-encrypted connection, the encrypted connection allowing access to a file server and the non-encrypted connection not allowing access to the file server but allowing access to the Internet and an email server. The claims clearly recite a level of detail not at all contemplated by the broad disclosure in Flint at column 2, lines 15-28.

Further the disclosure in Wood to tailoring credentials to current access requirements also does not address the specific features recited in the claims as noted above.[6]

In such further ways the disclosure in Wood is not believed to cure the deficiencies in Flint. Moreover, no teachings in the Microsoft Dictionary were cited with respect to, or are believed to cure, the deficiencies of Flint in view of Wood.

In view of these foregoing comments, applicants respectfully submit the claims as currently written distinguish over the applied art.

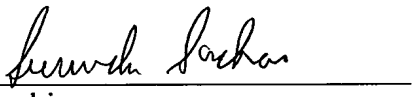
---

[5] Office Action of December 1, 2005, the paragraph bridging pages 2 and 6.
[6] Office Action of December 1, 2005, the middle of page 17.

As no other issues are pending in this application, it is respectfully submitted that the present application is now in condition for allowance, and it is hereby respectfully requested that this case be passed to issue.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



James J. Kulbaski
Registration No. 34,648
Surinder Sachar
Registration No. 34,423
Attorneys of Record

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)
JJK/SNS:sih

I:\ATTY\SNS\20's\203223\203223US-AM2.DOC